4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,268	10/07/2003	Anthony C. Fascenda	62922.4	3130

21967 7590 01/30/2007

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
NGUYEN, KHOI	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/679,268	Applicant(s) FASCENDA, ANTHONY C.
	Examiner Khoi Nguyen	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11/29/04 and 30/07/05*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 22 are pending

Claim Objections

2. Claim 11 is objected to for lack of antecedent basis:

- "Said a secret cryptographic key" line 7.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 7-8, 11 are rejected under 35 USC 112, second paragraph as being indefinite for failing to particularly point out and distinct claim the subject matter which applicant regards as the invention.

5. The following phrases are not clearly understood, rendering the corresponding claims vague and indefinite

   a. the phase "each set of authentication parameters" on line 3 of claim 7 and line 2 of claim 8 is not clearly understood whether it is referring to the additional sets of authentication parameters or any other set of authentication parameters. For the purpose of examining, it is treated as additional sets of authentication.

b. The phase "said a secret cryptographic key" on line 7 is not clearly understood whether it is referring to the first secret cryptographic key or any cryptographic key. For the purpose of examining, it is treated as a cryptographic key.

c. The phrase "said unique identifier" on line 8 is not clearly understood whether it is referring to identifier of the Access Point or computing device. For the purpose of examining, it is treated as the unique identifier associates with the Access Point.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 9, 16-17 and 20-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Whelan et al (US. PGPub No. 2004/0198220), hereafter "Whelan".

8. With regard to claim 1, Whelan discloses method of authenticating a computing device on a Wi-Fi communications network comprising the steps of:

obtaining an access point identifier (Fig. 1, item 28, [0032], lines 21-23, association list is downloaded that contains AP identifier for each sub-net indicates obtaining an access pointer identifier) at a computing device (Fig. 1, item mobile unit), wherein said access point identifier identifies an access point of a Wi-Fi communications network([0063], lines 1-3);

selecting, at said computing device (Fig. 1, item 28 mobile unit), a set of authentication parameters associated with said access point identifier ([0043], lines 5-8) ; and

implementing an authentication process employing said set of authentication parameters ([0049] lines 13-16, authenticate the access point reads on implementing an authentication process and the access point on the association list indicates authentication parameters).

9. With regard to claims 2 and 21, Whelan discloses access point identifier is a basic service set identifier (BSSID) ([0006], lines 1-5).

10. With regard to claim 3, Whelan discloses step of obtaining an access point identifier, comprises the step of receiving said basic service set identifier from said access point (Fig. 1, [0045] lines 12-14).

11. With regard to claim 9, Whelan discloses the step of permitting said computing device to access said Wi-Fi communications network via said access point if said authentication process results in a successful authentication of said computing device (Fig. 2a and 2b, [0049] lines 8-16).

12. With regard to claim 16, Whelan discloses each client device further includes a wireless communications transceiver to communicate with one of said one or more authentication device via a wireless channel (Fig. 1, [0082] lines 1-6).

13. With regard to claim 17, Whelan discloses wireless channel (Fig. 1, item 26) is an IEEE 802.11 wireless channel ([0004] lines 1-4).

14. With regard to claim 20, Whelan discloses each of the one or more unique sets of authentication parameters is associated with an access point identifier ([0043], lines 5-8).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 4-8, 10, 12, 18-19, and 22 are rejected under 35 USC 103(a) as being unpatentable over Whelan, and in view of Balogh (US PGPub. No. 2001/0023446), hereafter "Balogh".

17. With regard to claim 4, Whelan discloses set of authentication parameters ([0043], lines 5-8), but did not disclose set of authentication parameters are pre-stored in a tamper-resistant physical token.

Balogh, on the other hands, discloses set of authentication parameters are pre-stored in a tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that set of authentication parameters are pre-stored in a temper-resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

18. With regard to claim 5, Whelan does not disclose installing the tamper-resistant physical token at the computing device. However, Balogh discloses installing the tamper-resistant physical token at the computing device ([0030], lines 7-9).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan by installing the tamper-resistant physical token at the computing device, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

19. With regard to claims 6 and 22, Whelan does not disclose the tamper-resistant physical token is adapted to be inserted into a communications port at the computing device. However, Balgoh discloses the tamper-resistant physical token is adapted to be inserted into a communications port at the computing device ([0030] lines 7-9, card reader indicates a communication port).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that the tamper-resistant physical token is adapted to be inserted into a communications port at the computing device, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

20. With regard to claim 7, Whelan discloses one or more additional sets of authentication parameters ([0050] lines 4-5, temporary association list indicate one or more sets of authentication parameters), wherein each set of authentication parameters is associated with a unique access point identifier ([0051] lines 1-3).

However, Whelan does not disclose the tamper-resistant physical token further comprises one or more additional sets of authentication parameters, wherein each set of authentication parameters is associated with a unique access point identifier.

Balgogh, on the other hand, discloses the tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7) further comprises one or more additional sets of authentication parameters, wherein each set of authentication parameters is associated with a unique access point identifier.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan to include the tamper-resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

21. With regard to claim 8, Whelan discloses each of the unique access point identifiers is in relation to its associated set of authentication parameters (Fig. 1, item 34, [0042] 4-7).

However, Whelan does not discloses each of the unique access point identifiers is stored in said tamper-resistant physical token and in relation to its associated set of authentication parameters.

Balgogh, on the other hand, discloses each of the unique access point identifiers is stored in said tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7) and in relation to its associated set of authentication parameters.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that set of authentication parameters are pre-stored in a temper-resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

22. With regard to claim 10, Whelan discloses set of authentication parameters ([0043], lines 5-8), but does not disclose set of authentication parameters comprises a first secret cryptographic key.

However, Balogh discloses set of authentication parameters comprises a first secret cryptographic key (Fig. 2, WLAN-specific settings item, row 9, [0027] lines 12-15, WEPkeys indicates a first secret cryptographic key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that set of authentication parameters includes a secret cryptographic key, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

23. With regard to claim 12, Whelan disclose the unique identifier is a serial number ([0006], lines 3-4, BSSID uniquely identify an Access point indicates a serial number), but Whelan does not disclose a serial number of the tamper resistant physical token.

Balogh, on the other hand, discloses the tamper resistant physical token (Fig. 1, item SC, [0030] lines 4-7).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the authentication process method of Whelan by includes a serial number of the tamper resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

24. With regard to claim 18, Whelan discloses one or more authentication devices (Fig. 1, item 10) but does not disclose one or more authentication devices are Wi-Fi access points.

Balogh, on the other hand, disclose one or more authentication devices are Wi-Fi access points (Fig. 1, AP1-AP3).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the authentication process method of Whelan by including one or more authentication devices are Wi-Fi access points, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

25. With regard to claim 19, Whelan discloses at least two Wi-Fi access points (Fig. 1, Item 28) but does not disclose at least two Wi-Fi access points are associated with different Wi-Fi networks are associated with different Wi-Fi networks.

Balogh, on the other hand, discloses at least two Wi-Fi access points are associated with different Wi-Fi networks (Fig. 1, Item AP1-4 with NW1 and NW2).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the communication system of Whelan by including at least two Wi-Fi access points are associated with different Wi-Fi networks, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

26. Claims 11, 13-15 are rejected under 35 USC 103(a) as being unpatentable over Whelan, in view of Balogh, and further in view of Nevoux et al. (US Pat. No. 5661806), hereafter "Nevoux".

27. With regard to claim 15, Whelan discloses a communications system comprising: one or more authentication devices (Fig. 1, Item 10, [0074] lines 1-3)
one or more client devices (Fig. 1, item 28), one or more unique sets of authentication parameters ([0043], lines 5-8), wherein each set of authentication parameters is associated with one or more of said one or more authentication devices (Fig. 1, item 10); and a unique serial number ([0006], lines 3-4, BSSID uniquely identify an Access point indicates a serial number).

However, Whelan does not disclose each client device includes a unique tamper-resistant physical token comprising: a random number generator

Balogh, on the other hand, discloses each client device includes a unique tamper-resistant physical token (Fig. 1, item SC, [0030] lines 4-7) comprising: a random number generator.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the authentication process method of Whelan by includes a serial number of the tamper resistant physical token, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings (Balogh, [0007] lines 1-3).

Nevertheless, neither Whelan nor Balogh discloses each client device includes a unique tamper-resistant physical token comprising: a random number generator.

However, Neouvx discloses each client device includes a unique tamper-resistant physical token comprising: a random number generator (Fig. 2, VLR column, R1 and R2, col. 4, lines 50-51)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh to include each client device includes a unique tamper-resistant physical token comprising: a random number generator, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system

28. With regard to claim 11, Whelan discloses authentication process comprises the steps of: transmitting a first challenge (Fig. 2A, item 50, initiates association indicates first challenge), receiving a second challenge (Fig. 2A, item 66, since the outcome of the decision branch of Item 66 feed the response back to the MU indicating there are more AP available; it reads on second challenge), access point associate with a unique identifier ([0006], lines 1-5) in which generated and stored at access point (Fig. 1, item 20 - AP and 36 – MU association list)

However, Whelan does not disclose the first challenge comprises an encrypted first random number and a unique identifier associated with said computing device, said encrypted first random number being encrypted with said first secret cryptographic key.

Furthermore, Whelan does not disclose the second challenge comprises an encrypted second random number; the second random number generated and encrypted with a secret cryptographic key.

Balogh, on the other hand, discloses the first challenge comprises a unique identifier associate with said computing device (Fig. 1, Item SC, [0031] line 5-6) and a secret cryptographic key (Fig. 2, WLAN-specific settings item, row 9, [0027] lines 12-15).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Whelan such that set of authentication parameters for the first challenge communication to include a secret cryptographic key and a unique identifier associate with the device, as taught by Balogh to allow users to connect to a network without knowing what settings are needed and how to change the settings ([0007] lines 1-3).

However, neither Whelan nor Balogh discloses the encrypted first random number being encrypted with said first secret cryptographic key and an encrypted second random number; the second random number is generated and encrypted with a secret cryptographic key.

Nevoux, on the other hand, discloses the first challenge comprises an encrypted first random number (Fig. 2, SIM Column, R1, R1 being encrypted by an encryption function in the initial stage of authentication indicates first encrypted random number) and the encrypted first random number being encrypted with the first secret cryptographic key as indicated regarding to claim 10, above.

Nevoux, further discloses an encrypted second random number (Fig. 2 VLR column, SRES item, col.2 lines 62-64, AT is an encryption function that includes a second random number R2; thus indicating an encrypted second random number), the second random number is generated (Fig. 2, VLR column, R2) and encrypted with a secret cryptographic key as indicated regard to claim 10 above.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh with the authentication process comprises of an encrypted first random number that being encrypted with the first secret cryptographic key, and an encrypted second random number being encrypted with a secret encrypted key, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system.

29. With regard to claim 13, Whelan discloses the set of authentication parameters ([0043], lines 5-8), further comprises: a network (Fig. 1, item 18, [0042] lines 1-3)

However, neither Whelan nor Balogh discloses a network receive cryptographic key and a network send cryptographic key.

Nevoux, on the other hand, discloses a network receive cryptographic key (Fig. 2 VLR column, receiving SRES indicates receive cryptographic key) and a network send cryptographic key (Fig. 2, HLR Column, sending Ks which is a result of the AG encryption function, reads on send cryptographic key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh by including a network receive cryptographic key and a network send cryptographic key in the set of authentication parameters, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system.

30. With respect to claim 14, Whelan further discloses the first challenge (Fig. 2A, item 50, initiates association indicates first challenge) and the second challenge (Fig. 2A, item 66, since the outcome of the decision branch of Item 66 feed the response back to the MU indicating there are more AP available; it reads on second challenge), and decrypting the second challenge ([0075] lines 1-7).

However, neither Whelan nor Balogh discloses encrypting the first challenge with the network send cryptographic key; and decrypting the second challenge with the network receive cryptographic key.

Nevoux, on the hand, discloses encrypting said first challenge with said network send cryptographic key (Fig. 2, HLR column item Ks, sending Ks which is an encrypted cryptographic key from a network indicates network send cryptographic key) and network receive cryptographic key (Fig. 2 VLR column, receiving SRES indicates receive cryptographic key)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Whelan and Balogh to include in the authentication parameters further comprises the step of encrypting said first challenge with said network send cryptographic key, as taught by Nevoux to avoid unauthorized access from mobile stations of malicious intruders in a radio-based wireless LAN system.

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US PGPub. No. 2003/0095663 to Nelson et al. (Discloses generating a pair of WEP key by a network access point).

b. US PGPub No. 2004/0153553 to Chotkowski et al. (Discloses authentication between wireless device with central server).

c. US PGPub No. 2003/0061363 to Bahl et al. (Discloses managing roaming mobile users between network).

d. US Pat. No. 7028186 to Stenman et al. (Discloses creating, utilizing and managing security key in a WLAN between mobile user and access point).

e. US PGPub No. 2001/0048744 to Kimura (Discloses authentication method of an AP).

f. US Pat. No. 6980660 to Hind et al. (Discloses enabling wireless devices distributed in an enterprise with public key cryptography and machine UI to establish a secure channel).

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est)
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KN
Khoi Nguyen

Gilberto B

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100